The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

TLP: WHITE
Disclosure is not limited. Subject to standard copyright rules, TLP: WHITE information may be distributed without restriction.
http://www.us-cert.gov/tlp/

DATE(S) ISSUED:
11/12/2019

SUBJECT:
Multiple Vulnerabilities in VMware Products Could Allow for Remote Code Execution

OVERVIEW:
Multiple vulnerabilities have been discovered in VMWare Workstation, Fusion and ESXi, the most severe of which could allow for remote code execution. Successful exploitation of the most severe of these vulnerabilities could result in an attacker gaining the same privileges given to the host machine. Depending on the privileges ran with VMWare Workstation or Fusion, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than those who operate with administrative user rights.

THREAT INTELLIGENCE:
There are currently no reports of these vulnerabilities being exploited in the wild.

SYSTEMS AFFECTED:

- VMWare Workstation version 15.x prior to 15.5.1
- VMWare Fusion version 11.x prior to 11.5.1
- VMWare ESXi version 6.0.x, 6.5.x, 6.7.x

RISK:
Government:

- Large and medium government entities: **High**
- Small government entities: **Medium**

Businesses:

- Large and medium business entities: **High**
- Small business entities: **Medium**

Home users: Low

TECHNICAL SUMMARY:
Multiple vulnerabilities have been discovered in VMWare Workstation, Fusion and ESXi, the most severe of which could allow for remote code execution. Details of these vulnerabilities are as follows:

- VMware Workstation and Fusion contain an out-of-bound write vulnerability which exist in the e1000e virtual network adapter has been addressed. (CVE-2019-5541)

- VMware Workstation and Fusion contain an information disclosure vulnerability which exist in vmnetdhcp has been addressed (CVE-2019-5540)
- VMware Workstation and Fusion contain a denial of service vulnerability which exist in the RPC handler has been addressed (CVE-2019-5542)
- VMware Workstation and Fusion contain a denial of service vulnerability involving Machine Check Error on Page Size Change (CVE-2018-12207)
- VMware ESXi, Workstation, and Fusion contain a speculative-execution vulnerability involving TSX Asynchronous Abort (CVE-2019-11135)

Successful exploitation of the most severe of these vulnerabilities could result in an attacker gaining the same privileges given to the host machine. Depending on the privileges ran with VMWare Workstation or Fusion, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than those who operate with administrative user rights.

RECOMMENDATIONS:
The following actions should be taken:

- Apply appropriate patches or appropriate mitigations provided by VMware to vulnerable systems immediately after appropriate testing.
- Run all software as a non-privileged user (one without administrative rights) to diminish the effects of a successful attack.
- Remind all users not to visit untrusted websites or follow links provided by unknown or untrusted sources.
- Inform and educate users regarding threats posed by hypertext links contained in emails or attachments especially from untrusted sources.
- Apply the Principle of Least Privilege to all systems and services.

REFERENCES:

VMware:
https://www.vmware.com/security/advisories/VMSA-2019-0020.html
https://www.vmware.com/security/advisories/VMSA-2019-0021.html

CVE:
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-12207
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-11135
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-5540
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-5541
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-5542

Chris Watts
Security Operations Analyst
MS Department of Information Technology Services
601-432-8201 | www.its.ms.gov

iTS Mississippi Department of
Information Technology Services
3771 Eastwood Drive | Jackson, Mississippi 39211-6381

DISCLAIMER: This email and any files transmitted with it are confidential and intended solely for the use of the individual or entity to whom they are addressed. If you have received this email in error please notify the system manager. This message contains confidential information and is intended only for the individual named. If you are not the named addressee you should not disseminate, distribute or copy this e-mail. Please notify the sender immediately by e-mail if you have received this e-mail by mistake and delete this e-mail from your system. If you are not the intended recipient you are notified that disclosing, copying, distributing or taking any action in reliance on the contents of this information is strictly prohibited